UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

United States of America,

Plaintiff,

v.

D-2 Ricky Handschumacher,

Defendant. /

Case No.: 19-cr-20246
Honorable Denise Page Hood

GOVERNMENT'S SENTENCING MEMORANDUM

Ricky Handschumacher was a member of a group of hackers known as "The Community." Members of The Community engaged in a fraudulent scheme that exploited Internet security vulnerabilities through a method known as SIM hijacking. The scheme began with redirecting a victim's mobile phone number, which led to hackers seizing control of the victim's email and other online accounts. One goal of this scheme was the theft of cryptocurrencies, such as Bitcoin.

Over approximately two years, members of The Community stole over fifty million dollars' worth of cryptocurrency. Handschumacher personally participated in the theft of cryptocurrency valued at over seven million dollars.

Handschumacher's undisputed guideline range is 78 – 97 months. For the reasons stated in this memorandum, a sentence of 88 months incarceration—the midpoint of the range—followed by three years' supervised release, is "sufficient,

but not greater than necessary," pursuant to the purposes of 18 U.S.C. § 3553(a).

I. BACKGROUND

A. Introduction to Cryptocurrency

Cryptocurrencies, also known as virtual currencies or digital currencies, are online media of exchange. The most famous is Bitcoin, but many others exist—such as Litecoin and Ethereum. Like traditional currencies, they act as stores of value and can be exchanged for goods and services. They can also be exchanged for dollars. Unlike fiat currencies such as the dollar, however, they are untethered from the traditional banking system and neither issued nor backed by sovereign states. Their value depends solely on the law of supply and demand.

Cryptocurrencies' values fluctuate dramatically, but their popularity continues to increase. A 2015 survey found over 100,000 online merchants accepting Bitcoin.[1] That same year, between 80,000 and 220,000 Bitcoin transactions occurred each day, "representing over $50 million in estimated daily volume."[2]

As the popularity of cryptocurrencies has grown, hackers have honed strategies to steal them. Victims of cryptocurrency theft have limited recourse because cryptocurrency transactions are irrevocable—i.e., no bank or other central

[1] See Exhibit 1, Latham & Watkins LLP, Cryptocurrency: A Primer (2015).

[2] Id.

authority can reverse fraudulent transactions.

B. Introduction to SIM Hijacking

SIM hijacking, also known as SIM swapping, is an identity theft technique that exploits a near-ubiquitous cyber-security weakness: mobile phone numbers. Mobile phone numbers are, typically, associated with a single device and a single individual. This has transformed them—and their associated phones—into personal identification tools. Mobile phone numbers are frequently used as a means of authentication to access email, social media, banking, and other online accounts. Two-factor authentication ("2FA") protocols for many websites involve texting a security code to a mobile number. Password resets for online accounts are commonly executed via text messages to mobile numbers. For some online services, simply accessing the service via a mobile device associated with a particular assigned phone number suffices to gain access to an account.

This transformation of the mobile phone number from a means of communication to a means of identification parallels the unintended evolution of the social security number into a default national-ID number. Unsurprisingly, it has led to another corresponding evolution: hackers seeking to gain control over mobile phone numbers as a means to assume a victim's identity.

The vector for such an attack is typically the victim's mobile provider. Sometimes, the assault begins with social engineering: the attacker contacts a mobile

provider's customer service, pretends to be the victim, claims to have lost "their" phone, and then asks for "their" phone number to be associated with a new device. Alternatively, the attacker (or an associate) bribes a provider's representative to either transfer the victim's number to a new device or turn over data necessary to associate a new device with the victim's phone number. This technique is called SIM hijacking because it is often accomplished by reprograming a phone's SIM (Subscriber Identity Module) card. If the attack succeeds, phone calls and text messages intended for the victim are re-routed to the attacker instead.

However the hijacking is accomplished, the next steps by the attacker are the same. Once in control of the victim's mobile number, the attacker hacks into the victim's email by either (1) cracking (or stealing) the password and then requesting a 2FA code be sent via text message or (2) requesting that the password be reset via text message. The attacker then seizes control of additional online accounts by resetting passwords linked to the now compromised email address. Criminals have used this technique to drain bank accounts, steal cryptocurrency, steal compromising photographs, or simply to take over social media accounts with usernames a hacker covets and/or can sell.[3]

[3] Single letter social media accounts such as "@t" or "@x" are common targets. The hackers who stole the "@t" Instagram account claim to have sold it for approximately $40,000. See also Lorenzo Franceschi-Bicchierari,, *The SIM Hijackers, (2018), at* https://motherboard.vice.com/en_us/article/vbqax3/hackers-sim-swapping-steal-phone-numbers-instagram-bitcoin. Other social media accounts that have been targeted for takeover in this manner include "@rainbow" and "@sex."

C. The Community

"The Community" was a loosely organized network of computer hackers, many of whom engaged in SIM hijacking. The group's members discussed SIM hijacking on various online forums and over diverse channels of communication. Broader conversations—such as discussing the manner and means of attacks among The Community's members—typically took place on forums such as "OGUsers" and "Hackforums." Planning and execution of specific attacks usually took place via communication platforms such as Discord, Skype, Signal, Wickr, and Telegram.

A subset of the "The Community" that included defendant Ricky Handschumacher focused on using SIM hijacking to steal cryptocurrency. Members of this group had different roles. Some searched through online forums dedicated to cryptocurrencies, identifying potential victims and gathering the information (such as mobile phone numbers) necessary to initiate an attack. Others specialized in reprogramming SIM cards; often these individuals had contacts at mobile phone providers susceptible to bribes. Other members specialized in the actual account-takeovers and the transfers of funds.

II. OFFENSE CONDUCT

Ricky Handschumacher pleaded guilty to one count of Conspiracy to Commit Wire Fraud (18 U.S.C. § 1349). He participated in numerous SIM hijacking attacks in 2017 and 2018. The exact number of attacks (and their associated losses) is unknown, but Handschumacher does not dispute that he conspired to attack more than ten victims that suffered losses. The government has verified that Handschumacher personally participated in thefts resulting in losses of cryptocurrency valued at over seven million dollars (valued on the date of theft).[4] The charts below document the losses of each of these thefts, valuing the stolen cryptocurrencies both on the date of the theft and on the date of Handschumacher's guilty plea (October 18th, 2019).[5]

Victim S.B. (Date of theft: 05/03/2018)

Cryptocurrency	**Amount**	**Value: 5/03/18**	**Value: 10/18/19**
Ethereum	1242	$974,150.28	$221,299.56
Dash	9043.56835	$4,623,886.06	$627,352.34
		$5,598,036.34	$848,651.90

Victim D.M. (Date of theft: 05/15/2018)

Cryptocurrency	**Amount**	**Value: 5/15/18**	**Value: 10/18/19**
Ethereum	12.4980121	$9,236.66	$2,226.90
Metal	920.938262	$3,913.99	$295.55
Polymath	86,753.34	$103,236.48	$2,275.11
		$116,387.12	$4,797.56

[4] Stolen funds were split between co-conspirators. But a victim's loss, not a defendant's gain, is the proper measure of loss under the guidelines. USSG § 2B1.1 cmt. n. 3 (2018).

[5] Cryptocurrencies are valued at the maximum U.S. dollar value reached on the relevant dates

Victim S.S. (Date of theft: 05/16/2018)

Cryptocurrency	**Amount**	**Value: 5/16/18**	**Value: 10/18/19**
Bitcoin	70.01	$595,675.18	$569,770.08
Ethereum	1274.5	$905,149.90	$227,090.41
Dash	13.63	$5,851.63	$945.51
Litecoin	157.67	$22,176.29	$8,678.16
Polymath	209997	$220,496.85	$5,507.17
WAX	499999	$169,631.66	$12,902.47
RChain	4793	$7,716.73	$134.73
LOCIcoin	40746	$5,345.02	$40.30
		$1,967,146.57	$827,141.32

III. Restitution

The Government will submit a proposed order requesting that that the Court order restitution pursuant to Handschumacher's Rule 11 agreement. That agreement obliges him to pay victims restitution in the amount of the higher of two values: the value of the stolen cryptocurrency on the date of the theft, or its value on the date of his guilty plea.

In each instance in which the government has linked Handschumacher to a documented cryptocurrency loss, the value on the date of theft was greater than the value on the date of Handschumacher's plea (i.e., the value of the stolen cryptocurrency has dropped). Therefore, pursuant to the Rule 11 agreement Handschumacher is obligated to pay the following restitution:

Victim S.B.: $5,598,036.34

Victim D.M.: $116,387.12

Victim S.S.: $1,967,146.57

IV. Forfeiture

The United States seeks to forfeit the following assets ("Subject Assets") from Handschumacher as proceeds of the crime to which he has pleaded guilty, pursuant to 18 U.S.C. § 981(a)(1)(C) with 28 U.S.C. § 2461(c):

a) 38.06185149 Bitcoin seized from Ricky Handschumacher (approximate value of $309,762.95 as of October 18, 2019);

b) 900.46813354 Ethereum seized from Ricky Handschumacher (approximate value of $160,445.41 as of October 18, 2019);

c) 2017 Ford F-250 Platinum, VIN Number 1FT7W2BT4HEB32435;

d) 2018 Polaris Ranger XP All-Terrain Vehicle, VIN Number 3NSRTA871JG978010; and,

e) 2019 Polaris Highlifter RZRX All-Terrain Vehicle, VIN Number 3NSVFM99XJF945262.

Handschumacher agreed to forfeit his interest in the Subject Assets in his Rule 11 plea agreement. (Dkt. # 247). A Preliminary Order of Forfeiture was entered forfeiting the aforementioned assets from Handschumacher on May 27, 2020. (Dkt. # 82).

V. Guidelines Range

The government has calculated that Handschumacher's sentencing guidelines call for a term of imprisonment of 78 – 97 months. The defendant does not dispute this range.

This guideline range is based on a Base Offense Level of 7 (Guideline § 2B1.1) with the following undisputed enhancements:

- Loss of $3,500,000 or more, less than $9,500,000 (2B1.1(b)(1)) (+18);
- Ten or more victims (2B1.1(b)(2)(A)(i)) (+2);
- Sophisticated Means (2B1.1(b)(10)(C)) (+2); and
- Use of an illicit authentication feature (2B1.1(b)(11)(ii)) (+2).

This results in an Adjusted Offense Level of 31. The government acknowledges that Handschumacher has accepted responsibility for his crimes, and thus has reduced the Offense Level Total by three points to 28.

Defendant has no criminal history, which results in a Guideline Range of 78 to 97 months of imprisonment and a Fine Guideline Range of $25,000 to $250,000. The government is not requesting that the Court impose a fine because of the significant amount of mandatory restitution.

VI. Sentencing Factors

Title 18, United States Code, Section 3553(a), sets forth a number of factors the Court shall consider in sentencing the defendant. These factors are described below, numbered as corresponding to Section 3553(a):

(1) The nature and circumstances of the offense…

Defined by financial loss alone, Handschumacher's crimes are dramatic. He has acknowledged participating in thefts of cryptocurrency valued at over seven million dollars.

But the damages extend beyond dollars. It is noteworthy that Handschumacher's victims are individuals, as opposed to corporations. Not only does financial loss to an individual victim potentially cause greater harm than an equal loss to a corporate entity, but individual victims face collateral consequences as result of the type of crime committed by the defendant. Identity theft is pernicious. Reestablishing control of online accounts, restoring credit ratings, recovering from reputational damage (both personal and business related) take time, effort, and often money. The collateral consequences of losing control of one's email, online storage, social media, and financial accounts can linger for years.

…and the history and characteristics of the defendant;

Handschumacher engaged in deliberate and repeated criminal activity. This was not a crime of impulse; Handschumacher continued to take part in a long-

running, multi-million-dollar conspiracy despite the fact that he could have withdrawn at any time. His criminal activity continued even after he and co-conspirators stole over five-million dollars in cryptocurrency in a single SIM hijacking attack.

Handschumacher's crimes were motivated purely by greed. He was not driven to crime by dire financial straits. He is an intelligent, capable individual, and at the time of his crimes he was working full time as a municipal employee. As a savvy and sophisticated computer user, Handschumacher was aware of the damage he was causing his victims. Any claim to the contrary would be incredulous. He knew that havoc he was wreaking—and didn't care. Lining his pockets and purchasing luxury goods—including a $75,000 pickup truck—was more important to him than the damage done to his victims.

The government acknowledges that, since caught, Handschumacher has appeared contrite and remorseful.[6] But this change of heart, assuming it is genuine, is too late for his victims and should not impact his sentence beyond the three-point guideline adjustment for acceptance of responsibility recommended by the government.

[6] The government also acknowledges that the defendant attempted to cooperate by providing information in proffers that took place in the Eastern District of Michigan and in the District of South Carolina. Ultimately, however, no information provided by the defendant was actionable, and thus the government is not seeking a guidelines reduction for cooperation.

The defendant's age is also relevant to his sentencing. Handschumacher is now 27; at the time of his crimes, he was 25. While far from being an old man, the defendant was significantly older than his co-conspirators—many of whom were teens and several of whom were minors. Handschumacher was not a socially maladjusted teen-recluse. At the time of his crimes, he was a former all-state athlete, with a steady job, a stable relationship, and a child. Relative to his co-defendants, Handschumacher's comparative maturity should be taken to account when evaluating his culpability and fashioning his sentence.

(2) The need for the sentence imposed (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense; (B) to afford adequate deterrence; (C) to protect the public from further crimes of the defendant; and (D) to provide defendant with appropriate education or vocational training.

Handschumacher's punishment should take into account not only the scope and seriousness of his criminal conduct but also the need to deter future crimes—both by Handschumacher and by others. With respect to specific deterrence, Handschumacher obtained a significant sum of money from his crimes. Commensurately significant incarceration is therefore necessary to demonstrate to him the proverbial mantra that "crime does not pay."

The sentence must also function as a general deterrent. This is an especially relevant consideration in this case—computer crimes are difficult for the government to police, and cause billions of dollars in damages each year. Convicted

computer criminals should therefore face severe penalties as a deterrent to other potential offenders.

Computer intrusions and identity thefts often go undetected. Victims also frequently fail to report them. When computer crimes are brought to the attention of law enforcement, enormous resources are required to identify and pursue those responsible. Computer intrusions are also becoming more common, and they are doing more damage than ever. The FBI's Internet Crime Complaint Center (IC3) 2019 Computer Crime report tallied losses in excess of $3.5 billion from over 450,000 complaints of suspected internet crime. In 2020, reported losses exceeded $4.1 billion from a record 791,790, complaints. CipherTrace, a computer forensics company focused on cryptocurrency, estimated global losses from cryptocurrency theft in 2019 at $4.52 billion—up 160% from losses in 2018.

In our increasingly connected world, every citizen is exposed to computer crime. As more of our social lives and finances migrate online, each of us has more and more to lose. This is happening at the same time that committing computer crime is becoming easier—the necessary skills are increasingly common, and online tutorials make it simple for even those with rudimentary knowledge to do tremendous damage. Stemming this tide is beyond the power of criminal prosecutions alone, but law enforcement and the courts have a role to play. This

Court should therefore consider general deterrence as a significant factor in sentencing the defendant.

(3) The kinds of sentences available

Under 18 U.S.C. § 1349 (Attempt and Conspiracy), the maximum sentence is linked to the underlying offense, in this case 18 U.S.C. § 1343 (Wire Fraud). The maximum penalty is therefore twenty years imprisonment and/or a fine not to exceed $250,000.00.

(4) The sentencing range established by the Guidelines

As set forth above in Section IV, the appropriate sentencing range, pursuant to the U.S. Sentencing Guidelines is 78 to 97 months imprisonment. The range is based on an Adjusted Offense Level of 31 and a three-level adjustment for acceptance of responsibility, making his Total Offense Level 28. Handschumacher's criminal history is Category I.

(5) Pertinent policy statements issued by the Sentencing Commission

The government is unaware of any pertinent policy statement issued by the United States Sentencing Commission.

(6) The need to avoid unwarranted sentencing disparities among defendants with similar records found guilty of similar conduct

Prior to the instant case, the government is aware of no federal defendant being sentenced for crimes connected to SIM hijacking. However, a sentence

handed down by a state court in California is comparable to the penalty that the government seeks here.

Joel Ortiz, defendant in Santa Clara County (California) Superior Court Case No. C1894831, pleaded guilty to SIM hijacking crimes identical in nature to those committed by Handschumacher. Ortiz, in fact, participated with Handschumacher in the thefts from S.B., D.M. and S.S. The judge in that case assumed a loss of approximately $7.6 million dollars, and sentenced Ortiz to ten years in prison. Ortiz was not granted credit, however, for either acceptance of responsibility or cooperation.

This Court has already sentenced two of Handschumacher's co-defendants, Reyad Abbas and Colton Jurisic. Both of these defendants were sentenced to below guidelines terms of imprisonment. The government notes, however, that each of these defendants were 18 years old at the time of their crimes. As pointed out above, however, Handschumacher was 25 years old and thus considerably more mature.

(7) The need to provide restitution

Restitution is mandatory in this case, as dictated by the Mandatory Criminal Restitution Act codified at 18 U.S.C. § 3663A. The necessary restitution in this case is described above in Section III.

RECOMMENDATION

The government recommends that defendant Ricky Handschumacher be sentenced to a term of 88 months in prison followed by three years of supervised release. For the reasons stated herein, the government believes that this sentence is necessary to fulfills the aims of 18 U.S.C. § 3553(a). As described above, the focus of the government is on the nature and circumstances of the offence, the history and characteristics of the defendant, and the need for deterrence.

The government also requests that restitution and forfeiture be ordered as described above in Sections III and IV.

Respectfully submitted,

SAIMA MOHSIN
Acting United States Attorney

/s/ Timothy J. Wyse
Timothy J. Wyse
Assistant U.S. Attorney
(313) 226-9144
211 West Fort, Suite 2001
Detroit, Michigan 48226
Timothy.Wyse@usdoj.gov

November 2, 2021